

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-138663

(P2000-138663A)

(43) 公開日 平成12年5月16日 (2000.5.16)

(51) Int.Cl. ⁷	識別記号	F I	テマコード (参考)
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B 5 B 0 4 9
G 0 6 F 19/00		G 0 9 C 1/00	6 4 0 B 5 J 1 0 4
G 0 9 C 1/00	6 4 0	G 0 6 F 15/28	B
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 D

審査請求 有 請求項の数21 O L (全 10 頁)

(21) 出願番号 特願平10-310855

(22) 出願日 平成10年10月30日 (1998. 10. 30)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 愛場 豊和

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100079164

弁理士 高橋 勇

Fターム (参考) 5B049 AA05 BB36 CC05 DD01 DD05

EE03 EE09 FF02 FF03 FF04

GG04 GG07 GG08 GG10

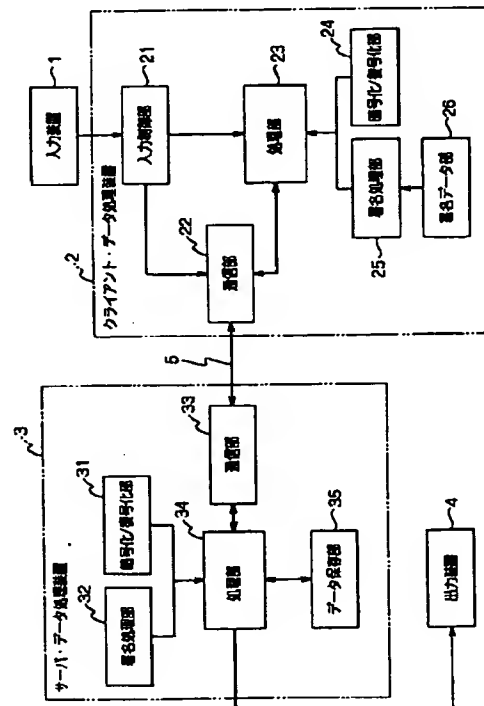
5J104 AA09 LA06 PA07 PA10

(54) 【発明の名称】 データ送受信システム

(57) 【要約】

【課題】 入札に必要な入札業務専用のソフトウェアを所持していない入札者にも、安全確実に入札データを投函させる。

【解決手段】 送信者は、入力装置1から送信すべき業務データを入力する。データ処理装置2は、プログラム制御により動作する第1の処理手段を具備し、通信回線5を介して一つ以上の処理装置3と結合されている。処理装置3は、プログラム制御により動作する第2の処理手段を具備し、前記第1の処理手段と前記第2の処理手段間で前記通信回線を介して前記業務データを送受信する。第1の処理手段は、初期状態において第2の処理手段の一部を構成している業務データ処理手段の一部又は全部の処理手続きを自己の内部に取り込み、該取り込まれたデータ処理手続きを用いて自己の現在のデータ処理手段に第2の業務データ処理手段を付加的に設置する手段を具備している。



【特許請求の範囲】

【請求項 1】 送信者側に設置され、送信すべき業務データを入力するためのデータ入力手段と、プログラム制御により動作する第 1 のデータ処理手段と、受信者側に設置され、通信回線を介して一つ以上の前記第 1 のデータ処理手段を結合したプログラム制御により動作する第 2 のデータ処理手段を具備し、前記第 1 のデータ処理手段と前記第 2 のデータ処理手段間で前記通信回線を介して前記業務データを送受信するために使用されるデータ送受信システムにおいて、

前記第 1 のデータ処理手段の初期状態における処理手続きは、

前記第 2 のデータ処理手段の一部として設定されている第 1 の業務データ処理手段の一部又は全部を構成している処理手続きを自己の内部に取り込み、

該取り込まれたデータ処理手続きを用いて自己の現在のデータ処理手段に第 2 の業務データ処理手段を付加的に設置することにより自己のデータ処理手段を完成する初期設定手段を有し、

前記初期設定手段の実施により完成された前記第 1 のデータ処理手段は、

前記付加的に設置された第 2 の業務データ処理手段に加えて、

前記第 2 の業務データ処理手段により処理された業務データを前記通信回線を介して前記第 2 のデータ処理手段に送出する第 1 の通信手段を有すること、

を特徴とするデータ送受信システム。

【請求項 2】 前記第 2 の業務データ処理手段は、前記データ入力手段から入力された前記業務データに電子署名を範疇とする署名データを付与する署名処理手段と、該署名データが付与された前記業務データを暗号化する暗号化手段を有すること、

を特徴とする請求項 1 記載のデータ送受信システム。

【請求項 3】 前記第 2 のデータ処理手段は、前記第 1 の通信手段から送出された前記業務データを所定のデータ保管場所に保存する入札データ保存手段と、該入札データ保存手段の実施後に、前記第 1 の通信手段に対して該入札データ保存手段の実施を完了した旨の通知をなす第 2 の通信手段を有し、かつ前記第 1 の業務データ処理手段として、前記第 1 の通信手段から送出された前記業務データを復号化する復号化手段と、該復号化された業務データの署名データを確認する署名照合手段と、前記復号化手段による復号が正常終了しなかった時に、その旨を表示する第 1 の表示手段と、前記署名照合手段において署名の確認が取れなかった時に、その旨を表示する第 2 の表示手段を有すること、

を特徴とする請求項 1 又は 2 記載のデータ送受信システム。

【請求項 4】 前記第 1 のデータ処理手段は、前記第 2 の通信手段から前記入札データ保存手段の実施を完了し

た旨の通知を受け取った時に、前記第 2 の業務データ処理手段を削除又は無効化する最終処理手段を有すること、

を特徴とする請求項 3 記載のデータ送受信システム。

【請求項 5】 前記第 1 の通信手段は、通信路用の暗号化／復号化手段を有すること、

を特徴とする請求項 1、2、3 又は 4 記載のデータ送受信システム。

【請求項 6】 前記第 2 の通信手段は、通信路用の暗号化／復号化手段を有すること、

を特徴とする請求項 3 又は 4 記載のデータ送受信システム。

【請求項 7】 前記業務データを入札業務に必要な入札データとしたこと、

を特徴とする請求項 1、2、3、4、5 又は 6 記載のデータ送受信システム。

【請求項 8】 送信者側に設置され、送信すべき業務データを入力するためのデータ入力ステップと、プログラム制御により動作する第 1 のデータ処理ステップと、受信者側に設置され、通信回線を介して一つ以上の前記第 1 のデータ処理ステップを結合したプログラム制御により動作する第 2 のデータ処理ステップを有し、前記第 1 のデータ処理ステップと前記第 2 のデータ処理ステップ間で前記通信回線を介して前記業務データを送受信するために使用されるデータ送受信方法において、前記第 1 のデータ処理ステップの初期状態における処理ステップは、

前記第 2 のデータ処理ステップの一部として設定されている第 1 の業務データ処理ステップの一部又は全部を構成している処理ステップを自己の内部に取り込み、該取り込まれたデータ処理ステップを用いて自己の現在のデータ処理ステップに第 2 の業務データ処理ステップを付加的に設置することにより自己のデータ処理ステップを完成する初期設定ステップを有し、

前記初期設定ステップの実施により完成された前記第 1 のデータ処理ステップは、

前記付加的に設置された第 2 の業務データ処理ステップに加えて、

前記第 2 の業務データ処理ステップにより処理された業務データを前記通信回線を介して前記第 2 のデータ処理ステップに送出する第 1 の通信ステップを有すること、

を特徴とするデータ送受信方法。

【請求項 9】 前記第 2 の業務データ処理ステップは、前記データ入力ステップから入力された前記業務データに電子署名を範疇とする署名データを付与する署名処理ステップと、該署名データが付与された前記業務データを暗号化する暗号化ステップを有すること、

を特徴とする請求項 8 記載のデータ送受信方法。

【請求項 10】 前記第 2 のデータ処理ステップは、前記第 1 の通信ステップから送出された前記業務データを

所定のデータ保管場所に保存する入札データ保存ステップと、該入札データ保存ステップの実施後に、前記第 1 の通信ステップに対して該入札データ保存ステップの実施を完了した旨の通知をなす第 2 の通信ステップを有し、かつ前記第 1 の業務データ処理ステップとして、前記第 1 の通信ステップから送出された前記業務データを復号化する復号化ステップと、該復号化された業務データの署名データを確認する署名照合ステップと、前記復号化手段による復号が正常終了しなかった時に、その旨を表示する第 1 の表示ステップと、前記署名照合手段において署名の確認が取れなかった時に、その旨を表示する第 2 の表示ステップを有すること、

を特徴とする請求項 8 又 9 記載のデータ送受信方法。

【請求項 11】 前記第 1 のデータ処理ステップは、前記第 2 の通信手段から前記入札データ保存ステップの実施を完了した旨の通知を受け取った時に、前記第 2 の業務データ処理ステップを削除又は無効化する最終処理ステップを有すること、

を特徴とする請求項 10 記載のデータ送受信方法。

【請求項 12】 前記第 1 の通信ステップは、通信路用の暗号化／復号化ステップを有すること、

を特徴とする請求項 8、9、10 又は 11 記載のデータ送受信方法。

【請求項 13】 前記第 2 の通信ステップは、通信路用の暗号化／復号化ステップを有すること、

を特徴とする請求項 10 又は 11 記載のデータ送受信方法。

【請求項 14】 前記業務データを入札業務に必要な入札データとしたこと、

を特徴とする請求項 8、9、10、11、12 又は 13 記載のデータ送受信方法。

【請求項 15】 送信者側に設置され、送信すべき業務データを入力するためのデータ入力ステップと、プログラム制御により動作する第 1 のデータ処理ステップと、受信者側に設置され、通信回線を介して一つ以上の前記第 1 のデータ処理ステップを結合したプログラム制御により動作する第 2 のデータ処理ステップを有し、前記第 1 のデータ処理ステップと前記第 2 のデータ処理ステップ間で前記通信回線を介して前記業務データを送受信するために実行されるプログラムを記録するコンピュータ読み込み可能な記録媒体において、

前記第 1 のデータ処理ステップの初期状態における処理手続きは、

前記第 2 のデータ処理ステップの一部として設定されている第 1 の業務データ処理ステップの一部又は全部を構成している処理手続きを自己の内部にダウンロードし、該ダウンロードされたデータ処理手続きを用いて自己の現在のデータ処理ステップに第 2 の業務データ処理ステップを付加的に設置することにより自己のデータ処理ステップを完成する初期設定ステップを有し、

前記初期設定ステップの実施により完成された前記第 1 のデータ処理ステップは、

前記付加的に設置された第 2 の業務データ処理ステップに加えて、

前記第 2 の業務データ処理ステップにより処理された業務データを前記通信回線を介して前記第 2 のデータ処理ステップに送出する第 1 の通信ステップとを有すること、

を特徴とするプログラムを記録するコンピュータ読み込み可能な記録媒体。

【請求項 16】 前記第 2 の業務データ処理ステップは、前記データ入力ステップから入力された前記業務データに電子署名を範疇とする署名データを付与する署名処理ステップと、該署名データが付与された前記業務データを暗号化する暗号化ステップを有すること、

を特徴とする請求項 15 記載のプログラムを記録するコンピュータ読み込み可能な記録媒体。

【請求項 17】 前記第 2 のデータ処理ステップは、前記第 1 の通信ステップから送出された前記業務データを所定のデータ保管場所に保存するステップを実行する入札データ保存ステップと、該入札データ保存ステップの実施後に、前記第 1 の通信ステップに対して該入札データ保存ステップの実施を完了した旨の通知をなす第 2 の通信ステップを有し、かつ前記第 1 の業務データ処理ステップとして、前記第 1 の通信ステップから送出された前記業務データを復号化する復号化ステップと、該復号化された業務データの署名データを確認する署名照合ステップと、前記復号化手段による復号が正常終了しなかった時に、その旨を表示する第 1 の表示ステップと、前記署名照合手段において署名の確認が取れなかった時に、その旨を表示する第 2 の表示ステップを有すること、

を特徴とする請求項 15 又 16 記載のプログラムを記録するコンピュータ読み込み可能な記録媒体。

【請求項 18】 前記第 1 のデータ処理ステップは、前記第 2 の通信手段から前記入札データ保存ステップの実行を完了した旨の通知を受け取った時に、前記第 2 の業務データ処理ステップを削除又は無効化する最終処理ステップを有すること、

を特徴とする請求項 17 記載のプログラムを記録するコンピュータ読み込み可能な記録媒体。

【請求項 19】 前記第 1 の通信ステップは、通信路用の暗号化／復号化ステップを有すること、

を特徴とする請求項 15、16、17 又は 18 記載のプログラムを記録するコンピュータ読み込み可能な記録媒体。

【請求項 20】 前記第 2 の通信ステップは、通信路用の暗号化／復号化ステップを有すること、

を特徴とする請求項 17 又は 18 記載のプログラムを記録するコンピュータ読み込み可能な記録媒体。

【請求項 21】前記業務データを入札業務に必要な入札データとしたこと、
を特徴とする請求項 15 乃至 20 のいずれか 1 項に記載のプログラムを記録するコンピュータ読み込み可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データ送受信システムに関し、とりわけ入札業務等を例に取れば、入力すべき入札データを、入札者側（以下、「クライアント」と呼称することがある）が通信回線（例えばインターネット等）を利用して遠隔地にある入札管理者側に送信する必要がある時に、入札者側が入札に必要な入札業務専用のソフトウェアを所持していない場合にも、安全確実に入札データを投函できるようにしたデータ送受信システムを提供するものである。

【0002】

【従来の技術】従来の入札システムの一例としては、特開平 7-21280 号公報に記載されているようなシステムが見られるが、該公報に記載されている入札システムは、入札業務専用のシステムとして構築されているが、入札者が入札システムが設置されている入札管理者側の場所まで出向き、入札を行うシステムである。

【0003】但し、従来のデータ送受信システムは、例えば、入札業務において入札者が入札データを送信し、受信元の入札管理者が該入札データを受信して、保管や表示等の業務を遂行するための電子入札システムとしても、既に使用されている。

【0004】その一例としては、各市場に設置されたファクシミリから入力された入札情報をコンピュータでソーティング処理して応札者側のコンピュータ端末に送信し、これを見た応札者の応札情報をコンピュータでソーティング処理して上記各市場のファクシミリに送信し、各市場では、上記送られて来た応札情報を見て落札者を決定する入札出荷システムが、特開平 3-1274 号公報に開示されている。

【0005】さらに、出荷者が所定の項目をホストコンピュータに送信し、ホストコンピュータは該送信された情報を整理し、購入者は該整理された応札情報を参照して、発注情報をホストコンピュータに送信し、入札締切り後に、一定の優先順位に基づいてホストコンピュータにより落札処理する競売システムが、特開平 9-171531 号公報に開示されている。

【0006】

【発明が解決しようとする課題】ところで、従来の技術には次のような問題点があった。第 1 の問題点は、上記の特開平 7-21280 号公報に記載されているシステムを例にとると、入札を行うために、入札者が、入札管理者側のシステムに属する機器設置場所まで赴かなくてはならないことである。すなわち、このタイプの入札シ

ステムでは、通信回線（例えば広義又は狭義のインターネット網等）の利用については何ら考慮されていない。

【0007】第 2 の問題点は、上記の特開平 9-171531 号公報に開示されているようなシステムを例にとると、システム専用端末を設置する必要があることである。すなわち、このタイプの入札システムでは、通信回線網（例えば広義又は狭義のインターネット網等）を利用して必要なソフトウェアをダウンロードして使用するということが試みられていない。

【0008】第 3 の問題点は、上記の特開平 3-1274 号公報に開示されているようなシステムを例にとると、ファクシミリで送信すべきデータの項目が入札業者の仲間内だけで規定されたものであり、かつ一般のファクシミリ通信網を利用するために、セキュリティ上の問題が解決されていないことである。

【0009】

【発明の目的】本発明は、以上のような従来のデータ送受信システムにおける問題点に鑑みてなされたものであり、送信者側が業務データの送信に必要な業務専用のソフトウェアを所持していない場合にも、安全確実に業務データを送信できるデータ送受信システムを提供することを目的とする。

【0010】

【課題を解決するための手段】上記の課題を解決するために、本発明に係るデータ送受信システムは、「送信者側に設置され、送信すべき業務データを入力するためのデータ入力手段と、プログラム制御により動作する第 1 のデータ処理手段と、受信者側に設置され、通信回線を介して一つ以上の前記第 1 のデータ処理手段を結合したプログラム制御により動作する第 2 のデータ処理手段を具備し、前記第 1 のデータ処理手段と前記第 2 のデータ処理手段間で前記通信回線を介して前記業務データを送受信するために使用されるデータ送受信システムにおいて、前記第 1 のデータ処理手段の初期状態における処理手続きは、前記第 2 のデータ処理手段の一部として設定されている第 1 の業務データ処理手段の一部又は全部を構成している処理手続きを自己の内部に取り込み、該取り込まれたデータ処理手続きを用いて自己の現在のデータ処理手段に第 2 の業務データ処理手段を付加的に設置することにより自己のデータ処理手段を完成する初期設定手段を有し、前記初期設定手段の実施により完成された前記第 1 のデータ処理手段は、前記付加的に設置された第 2 の業務データ処理手段に加えて、前記第 2 の業務データ処理手段により処理された業務データを前記通信回線を介して前記第 2 のデータ処理手段に送出する第 1 の通信手段を有することを特徴とするデータ送受信システム」

（請求項 1）を特徴とし、これにより上記目的を達成することができる。

【0011】さらに、上記データ送受信システムにおい

て、

・前記第2の業務データ処理手段は、前記データ入力手段から入力された前記業務データに電子署名を範疇とする署名データを付与する署名処理手段と、該署名データが付与された前記業務データを暗号化する暗号化手段を有すること（請求項2）、

【0012】・前記第2のデータ処理手段は、前記第1の通信手段から送出された前記業務データを所定のデータ保管場所に保存する入札データ保存手段と、該入札データ保存手段の実施後に、前記第1の通信手段に対して該入札データ保存手段の実施を完了した旨の通知をなす第2の通信手段を有し、かつ前記第1の業務データ処理手段として、前記第1の通信手段から送出された前記業務データを復号化する復号化手段と、該復号化された業務データの署名データを確認する署名照合手段と、前記復号化手段による復号が正常終了しなかった時に、その旨を表示する第1の表示手段と、前記署名照合手段において署名の確認が取れなかった時に、その旨を表示する第2の表示手段を有すること（請求項3）、

【0013】・前記第1のデータ処理手段は、前記第2の通信手段から前記入札データ保存手段の実施を完了した旨の通知を受け取った時に、前記第2の業務データ処理手段を削除又は無効化する最終処理手段を有すること（請求項4）、

【0014】・前記第1の通信手段及び／又は前記第2の通信手段は、通信路用の暗号化／復号化手段を有すること（請求項5、16）、

【0015】・前記業務データを入札業務に必要な入札データとしたこと（請求項7）、を特徴とする。

【0016】また、上記の課題を解決するために、本発明に係るデータ送受信システムは、請求項1乃至6に係るデータ送受信システムに使用されることを特徴とするデータ送受信方法を提供している（請求項8乃至14）。

【0017】さらに、上記の課題を解決するために、本発明に係るデータ送受信システムは、請求項8乃至14に係るデータ送受信方法に係る各ステップを実行するプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体を提供している（請求項15乃至21）。

【0018】以下、本発明の作用を説明する。本発明に係るデータ送受信システムは、送信者側に設置された入力装置から入力された業務データを、通信回線（例えば広義又は狭義のインターネット等）を使用して遠隔地に設置された受信者側に送信するに際して、送信者側が上記業務データの送信に必要な業務専用のソフトウェアを所持していない場合にも、安全確実に上記業務データを送信できるようにしている。

【0019】図1において、サーバ・データ処理装置3と、サーバ・データ処理装置3とは別の場所（遠隔地）

に設置されているクライアント・データ処理装置2とは、通信回線5（例えば広義又は狭義のインターネット等）を利用して接続することが可能な状況にある。また、クライアント・データ処理装置2は、初期状態においては、図2に示すクライアント・データ処理装置2の構成を取る。

【0020】この時、送信者が入力装置1から業務データを入力すると、クライアント・データ処理装置2の入力制御部21が、通信部22を介したサーバ・データ処理装置3の通信部33との接続を実施し、暗号化／復号化部31と署名処理部32と処理部34に存在する一部又は全部の処理手続きを、クライアント・データ処理装置2へダウンロードする。

【0021】上記ダウンロードされた暗号化／復号化部31と署名処理部32と処理部34の処理手続きは、それぞれ暗号化／復号化部24と署名処理部25と処理部23として、クライアント・データ処理装置2に設置され、下記の動作をする。処理部23は、入力装置1から入力された業務データを処理し、該業務データを通信部22を介してサーバ・データ処理装置3へ送信する。

【0022】この時、クライアント・データ処理装置2に上記設置された署名データ部26から、署名データ（例えば電子署名等）を、上記入力された業務データへ添付することにより、上記入力された業務データの認証性（誰が作成したのか明確にすること）を高めている。

【0023】さらに、上記送信途中において、上記業務データの内容を盗聴（盗み見）されたり改竄されることを防止するために、暗号化／復号化部24を使用して、上記業務データを暗号化した後にデータを送信することにより、高い信頼性と機密性を有する業務の処理を可能としている。

【0024】また、上記業務のための処理の終了後に、クライアント・データ処理装置2の構成から、処理部23と暗号化／復号化部24と署名処理部25とを自動的に削除し、クライアント・データ処理装置2の構成を図2の初期状態に戻している。これにより、クライアント・データ処理装置2自体には上記業務を実施するための特別な処理部が予め持たされていなくても、上記業務のための処理を遂行することを可能にしている。

【0025】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。

（第1の実施の形態）図1は、本発明の第1の実施の形態に係るデータ送受信システムの全体構成を示すブロック図である。図2は、本発明の第1の実施の形態に係るデータ送受信システムの初期状態における構成を示すブロック図である。以下、本実施の形態に係るデータ送受信システムを、電子入札システムを例に取って説明する。

【0026】クライアントが入札データを入力するためのキーボード等の入力装置1と、プログラム制御により動作するクライアント・データ処理装置2と、クライアント・データ処理装置2と通信回線5により結合され、かつ上記入札データの保存等の制御をなすサーバ・データ処理装置3と、ディスプレイ装置や印刷装置等で構成されて上記入札データを出力する出力装置4を含む。

【0027】図1、図2に示す入力装置1とクライアント・データ処理装置2の組は、本実施の形態としては、只一組だけが通信回線5を介してサーバ・データ処理装置3と結ばれているが、一般には不特定多数の入札者に対応する複数の組が、通信回線5を介してサーバ・データ処理装置3と結ばれ得る。

【0028】クライアント・データ処理装置2は、初期状態時においては、図2に示すように、入力制御部21と、通信部22と、署名データ部26のみを備えているが、入力装置1から入札データが入力されることによって、サーバ・データ処理装置3から処理部34と、暗号化／復号化部31と、署名処理部32との処理プログラムがクライアント・データ処理装置2内にダウンロードされ、上記それぞれの処理プログラムが、処理部23と、暗号化／復号化部24と、署名処理部25を構成する処理プログラムとなる。すなわち、クライアント・データ処理装置2の処理部23と、暗号化／復号化部24と、署名処理部25は、上記ダウンロードの実行を契機としてクライアント・データ処理装置2内に設定される。

【0029】入力制御部21は、入力装置1から入力された上記入札データの存在を確認した後、通信部22を介して、上記によって、処理部34と、暗号化／復号化部31と、署名処理部32を、ダウンロードするように制御し、該ダウンロード後、上記入力された入札データを処理部23へ引き渡す。通信部22は、サーバ・データ処理装置3と通信回線5（例えば広義又は狭義のインターネット等）を介して、データの授受を行う。

【0030】処理部23は、入力された入札データについて、データの認証性を高めるために、署名処理部25を呼び出し、署名処理部25を使用して署名データ（例えば電子署名等）を添付する。また、通信経路でのデータ内容の改竄、盗聴（盗み見）を防止するために暗号化／復号化部24を呼び出し、暗号化／復号化部24を使用して上記入力された入札データを暗号化する。暗号化／復号化部24は、上記処理部23から与えられた入札データを、所定の方法（例えばRSA等）により暗号化する。

【0031】署名処理部25は、入力されたデータに署名データ（例えば電子署名等）を添付するために、署名データ部26を呼び出し、署名データを受け取る。署名データ部26は、予め作成されている署名データ（例えば電子署名等）を管理し、署名処理部25の要求によ

り、必要な署名データを引き渡す。

【0032】サーバ・データ処理装置3は、暗号化／復号化部31と、署名処理部32と、通信部33と、処理部34と、データ保存部35を備えている。

【0033】通信部33は、クライアント・データ処理装置2と通信回線5を介してデータのやりとりを行う。

【0034】処理部34は、通信回線5を介してクライアント・データ処理装置2から送信されてきた入札データについて、該データを保存するために、データ保存部35を呼び出し、データを引き渡すと共に、上記入札データの復号化を行うために、暗号化／復号化部31を呼び出し、また、署名データの確認を行うために、署名処理部32を呼び出し、正しい署名データ（例えば電子署名等）が添付されていることを署名処理部32を使用して調べる。また、上記入札データが正しく処理された場合には、該入札データ等を出力装置4に表示する。しかしながら、入札データの復号化が正しくなされない場合や、署名データが正しくない場合には、不正である旨のメッセージ等を出力装置4に表示する。

【0035】暗号化／復号化部31は、与えられたデータを所定の方法（例えばRSA等）により、暗号化されたデータを元に戻す復号化を行う。

【0036】署名処理部32は、与えられたデータに添付されている署名データ（例えば電子署名等）が正しいか否かを検証する。このため、復号化した元データから署名データ（例えば電子署名等）を作成し、入力された入札データに添付されている署名データ（例えば電子署名等）と比較、検証を行う。

【0037】図3は、本発明の第1の実施の形態に係るデータ送受信システムの全体動作を説明するためのフローチャートである。以下、図1、2を参照しつつ、図3に示すデータ送受信システムの全体動作を説明する。

【0038】まず、ステップA1では、入力装置1から入力制御部21に入札データが入力される。これにより直ちに、ステップA2で、入力制御部21は、通信部22、通信回線5、通信部33を介してサーバ・データ処理装置3と通信可能な状態を確立する。さらに、ステップA3で、サーバ・データ処理装置3の処理部34と、暗号化／復号化部31と、署名処理部32との処理プログラムをクライアント・データ処理装置2にダウンロードし、該ダウンロードされた処理プログラムそれぞれを、クライアント・データ処理装置2内の処理部23と、暗号化／復号化部24と、署名処理部25を構成する処理プログラムとして実装する。

【0039】次に入力制御部21は、上記入力された入札データを処理部23に引き渡し、ステップA4で、処理部23は、該入札データに対しての認証性を高めるための署名データ（例えば電子署名等）を入札データへ添付するために、署名処理部25を呼び出し、署名処理部25を利用して署名データ（例えば電子署名等）を添付

する。この時、署名処理部 25 は、予め作成された署名データ（例えば電子署名等）を管理している署名データ部 26 を呼び出し、対象となる署名データ（例えば電子署名等）を署名データ部 26 から読み込む。署名データ部 26 は自身が管理している署名データ（例えば電子署名等）を署名処理部 25 へ受け渡す。

【0040】次に、ステップ A5 で、処理部 23 は、通信経路でのデータ内容の改竄、盗聴（盗み見）を防止のために暗号化／復号化部 24 を呼び出し、暗号化／復号化部 24 を利用して入札データ（署名データ含む）を暗号化する。次に、ステップ A6 で、処理部 23 は、上記暗号化された入札データを通信部 22 及び通信部 33 を介してサーバ・データ処理装置 3 へ送信し、

【0041】ステップ A7 にて、処理部 34 が上記暗号化された入札データを受信する。ステップ A8 では、上記データを受信した処理部 34 は、該データの保存を行うために、データ保存部 35 を呼び出し、データ保存部 35 を使用して該データの保存を行う。データ保存部 35 は、上記データをサーバ・データ処理装置 3 の所定の保存場所（図示は省略）へ保存し、

【0042】ステップ A9 にて、保存済である旨の通知を処理部 34 へ受け渡す。ステップ A10 では、上記保存済である旨を受け渡された処理部 34 は、通信部 33 及び通信部 22 を介して、上記と同じ通知を処理部 23 へ受け渡す。（これにより、クライアント・データ処理装置 2 では、上記保存された旨の通知を受信した処理部 23 が、処理部 23 と、暗号化／復号化部 24 と、署名処理部 25 とを削除（若しくは無効化）することになる。）

【0043】ステップ A11 では、処理部 34 は更に、上記受信され、かつ暗号化された入札データを復号するために、暗号化／復号化部 31 を呼び出し、暗号化／復号化部 31 を使用して暗号化された入札データを復号する。暗号化／復号化部 31 は、上記暗号化された入札データを復号する。該復号が正しく行われなかった場合には、暗号化／復号化部 31 は、処理部 34 へ復号が正しく行われなかった旨を通知する。ステップ A14 では、上記復号が正しく行われなかった旨を受け渡された処理部 34 は、復号化不能を判断し、復号化不能を示すメッセージ等を出力装置 4 に表示する。

【0044】上記の復号が正しく行われた場合は、ステップ A12 で、処理部 34 は、上記復号された入札データに添付されている署名データ（例えば電子署名等）を確認するために、署名処理部 32 を呼び出し、署名処理部 32 を使用して署名データ（例えば電子署名等）を確認する。署名処理部 32 は署名データ（例えば、電子署名、等）を確認して署名データ（例えば電子署名等）が正しくなかった場合、署名処理部 32 は処理部 34 へ署名データが正しくなかった旨を通知する。

【0045】ステップ A14 では、署名データ（例えば

電子署名、等）が正しくなかった旨を通知された処理部 34 が、署名データ不正が存在することを判断し、署名データ不正を示すメッセージ等を出力装置 4 に表示する。さもなく、署名データが正しく確認された場合は、ステップ a13 にて、処理部 34 は、上記入札データを、メッセージ等の形式に含めて出力装置 4 に表示する。

【0046】（第 2 の実施の形態）図 4 は、本発明の第 2 の実施の形態に係るデータ送受信システムの全体構成を示すブロック図である。図 4 に示す構成を参照すると、本実施の形態に係るデータ送受信システムは、図 1 に示された第 1 の実施の形態におけるデータ送受信システムの全体構成に比較すると、クライアント・データ処理装置 42 側に通信路用暗号化／復号化部 27 が付加され、サーバ・データ処理装置 43 側に通信路用暗号化／復号化部 36 が付加されている点が異なっている。

【0047】本実施の形態では、通信路用暗号化／復号化部 27 と通信路用暗号化／復号化部 36 とが、通信路上を流れるデータ自体を、上記したダウンロード情報も含めて暗号化し、盗聴（盗み見）され改竄されることを防止する。

【0048】これにより、各処理装置内での暗号化の他に、通信路上でも暗号化が実施されるので、2 重の暗号強度を持つという新たな効果が得られる。

【0049】なお、図 3 のフローチャートで示したプログラムなど、処理装置に上記の処理を行わせるためのプログラムは、CD-ROM などのコンピュータ読み取り可能な記録媒体に格納して配付してもよい。そして、パーソナル・コンピュータ、汎用コンピュータを範疇に含むコンピュータが、上記記録媒体から上記プログラムを読み出して、実行するものとしてもよい。

【0050】

【発明の効果】以上に説明したとおり、本発明に係るデータ送受信システムに依れば、クライアント・データ処理装置が入札業務専用のソフトウェアを予め設定されていなくても（すなわち入札業務専用のソフトウェアがインストールされていなくても）、不特定多数のクライアントが入札を実施することが可能となる。すなわち、サーバ・データ処理装置に通信回線（例えば広義又は狭義のインターネット等）を通して接続できさえすれば、誰でも、どこからでも入札業務を行うことが可能となる。その理由は、クライアントによる入札業務に際して、該入札業務に必要なソフトウェア一式を、該入札業務を行う時にのみ、クライアント・データ処理装置内にダウンロードし、入札業務を行えるためである。また、上記入札業務に必要な入札データの送信に先立って、該入札データは暗号化され、かつ該暗号化の仕組みを、クライアントを含む一般人にまで公開する必要がないので、上記入札データのセキュリティ上の安全性を確実にすることができる。さらに、上記入札業務に必要な入札データの

通信路上においても、通信路用暗号化／復号化部を付加することにより、上記入札データのセキュリティ上の安全性を一層確実にすることが可能となり、また、該付加された通信路用暗号化／復号化部は、上記ソフトウェア一式のダウンロードにおいても使用することができるので、入札業務のセキュリティ上の安全性をも確実にすることができる。

【図面の簡単な説明】

【図 1】 本発明の第 1 の実施の形態に係るデータ送受信システムの全体構成を示すブロック図である。

【図 2】 本発明の第 1 の実施の形態に係るデータ送受信システムの初期状態における構成を示すブロック図である。

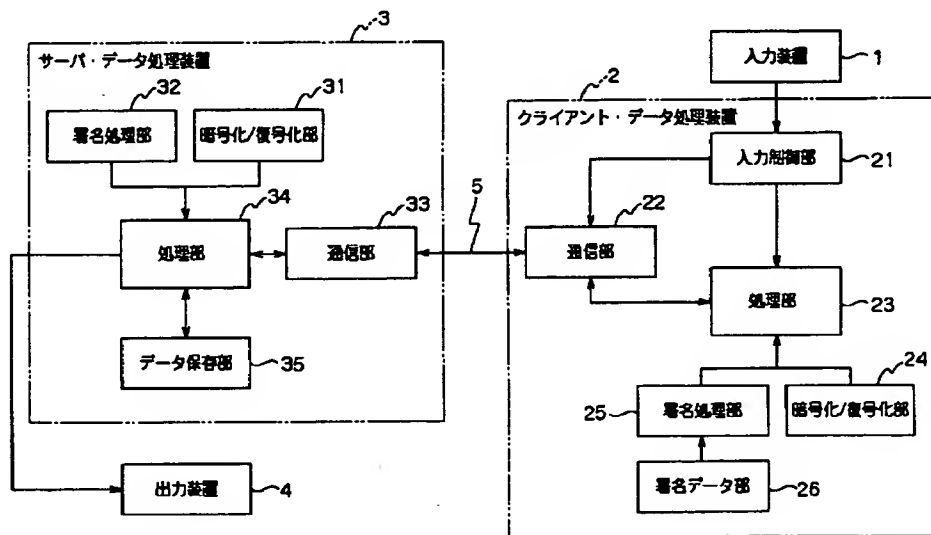
【図 3】 本発明の第 1 の実施の形態に係るデータ送受信システムの全体動作を説明するためのフローチャートである。

【図 4】 本発明の第 2 の実施の形態に係るデータ送受信システムの全体構成を示すブロック図である。

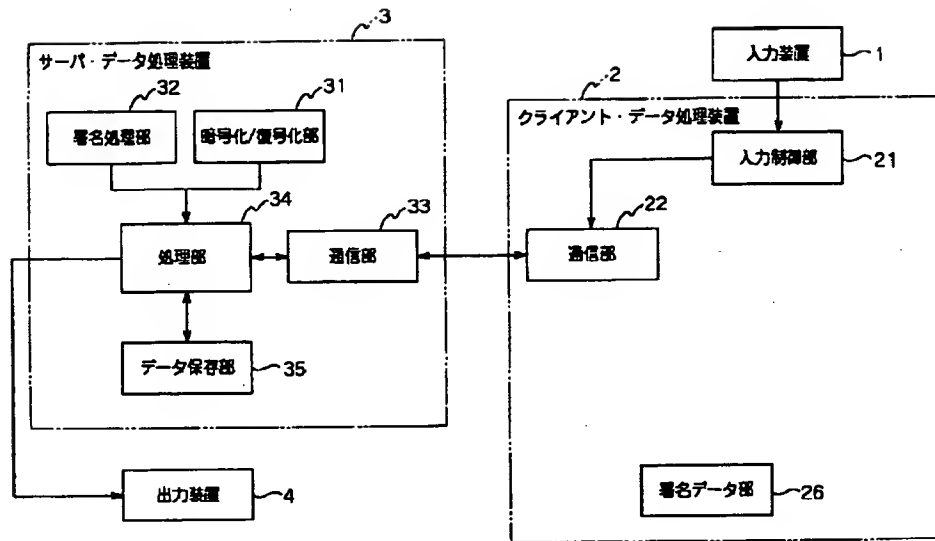
【符号の説明】

- 1 入力装置
- 2, 42 クライアント・データ処理装置
- 3, 43 サーバ・データ処理装置
- 4 出力装置
- 5 通信回線
- 21 入力制御部
- 22, 33 通信部
- 23, 34 処理部
- 24, 31 暗号化／復号化部
- 25, 32 署名処理部
- 26 署名データ部
- 27, 36 通信路用暗号化／復号化部
- 35 データ保存部

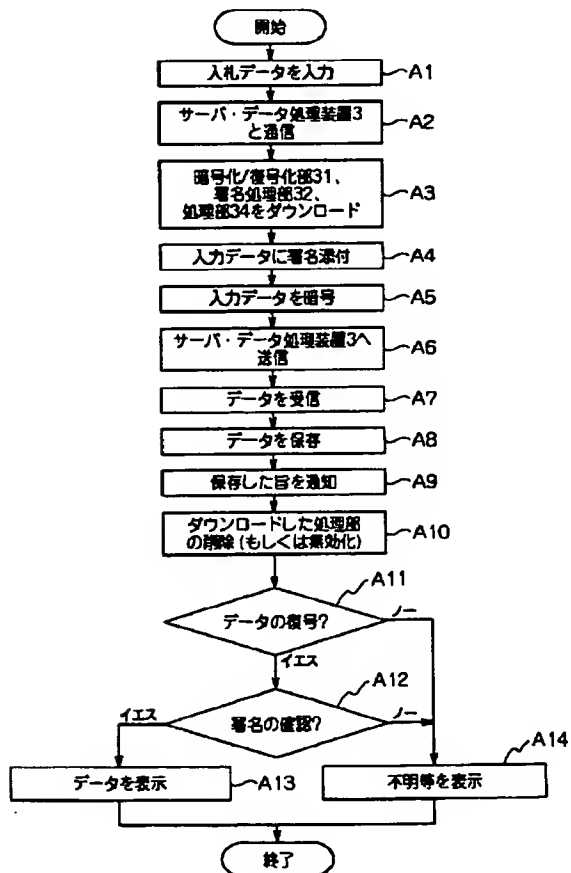
【図 1】



【図2】



【図3】



【図 4】

